Security Management of Cyber Physical Control Systems
July 2016-June 2019

Year 2 Mid-Year Report

State Board of Education
Higher Education Research Council
Idaho Global Entrepreneurial Mission (IGEM) Initiative Grant

Grant Number IGEM17-001

University of Idaho, College of Engineering

Project Director and PI: Larry Stauffer, Dean

Co-PI's: Fredrick Sheldon, Chair and Professor, Computer Science
Brian Johnson, SEL Endowed Chair, Electrical & Computer Engineering
Michael Haney, Assistant Professor, Computer Science
Daniel Conte de Leon, Assistant Professor, Computer Science

Executive Summary

Cyber-attacks and intrusions are nearly impossible to reliably prevent given the openness of today's networks and the growing sophistication of advanced threats. Knowing the vulnerabilities is not adequate, as the evolving threat is advancing faster than traditional cyber solutions can counteract. Accordingly, the practice of cyber security should focus on ensuring that intrusion and compromise do not result in business damage or loss through more resilient solutions. We are creating a platform to facilitate and build complementary and multidisciplinary R&D capabilities to address these pressing problems. Our platform will incubate innovative products and services for safeguarding cyber physical control systems (CPCSs) that are ubiquitous and underpin key sectors of our economy. Early participation of industry will aid in vetting promising technologies. Better methods for assessment combined with more resilient systems design will safeguard against potentially immense economic impact currently being faced by Idahoan stakeholders.

Idaho SBOE Contact:
Caron Howell
(208) 332-1563
Carson.howell@osbe.idaho.gov

Security Management of Cyber Physical Control Systems
July 1-December 31, 2017

Table of Contents

I. Summary of Project Accomplishments and Plans

This report provides the status of the project titled "Security Management of Cyber Physical Control Systems" which is an Idaho Global Entrepreneurial Mission (IGEM) Initiative Grant # IGEM17-001 sponsored by the Higher Education Research Council (HERC) of the Idaho State Board of Education (ISBOE). We are concluding the first eighteen-months of this three-year project and this report provides an update of progress during the time period of (July 1-December 31, 2017).

During the next six-month period, January 1-June 30, 2017, we plan to continue with our work plan as described in the proposal. Specifically we plan to complete the hiring of faculty and graduate students and place six student interns with industry partners. With regard to infrastructure enhancements we plan to complete the equipment installations in the power systems laboratory and start installation of the node in Coeur d' Alene. We will also make preparations for the third and final year of this project.

II. Budget Expenditures

Expenditures July 1 - December 30, 2017			
Category	Approved	Expenditur	Remaining	Notes
Salaries	$ 460,715	$224,278	$236,437	faculty and students
Fringe Benefits	$ 128,732	$ 54,145	$ 74,587	faculty and students
Travel	$ 10,000	$ 5,836	$ 4,164	
Operating	$ 78,153	$ 9,093	$ 69,060	saving for upcoming search expenses
Capital Outlay	$ -	$ -	$ -	
Tuition	$ 22,400	$ 11,974	$ 10,426	
Total	$ 700,000	$305,326	$394,674	

III. Demonstration of Economic Development/Impact

In this section we detail our accomplishments, organized by the four Objectives of the project.

(1) Strengthen our capacity by adding key faculty and enhancing laboratories.

In the second six months of 2017 we made substantial progress on laboratory enhancements, building collaborations, and producing research results. We added a new faculty member from last year's search process and reassigned the time of an existing faculty member to make progress on the goals of the project. We also continued the search process for the final two faculty positions called for in the proposal with on-site interviews scheduled for January. We also hired two PhD graduate students. A summary is as follows:

III.1.A Faculty Searches

Our work plan calls for the hiring of four new faculty members. We now have two of these faculty working. The latest hire is professor Dakota Roberson. Dr. Roberson earned a PhD in Electrical Engineering from the University of Wyoming in 2017. During his studies, he was also a half-time intern for Sandia National Laboratories. Being located in our program in Idaho Falls is an excellent fit for his national laboratory background and is already helping us in our work with the Idaho National Laboratory. His area of expertise is in wide-area damping control to control the effects of asymmetric time delay in geographically disparate locations, impact on coupling due to sensor/output collocation issues, and forced oscillations in the wide-area damping control environment. These situations matter because grid operators consider all of these limitations as they develop control systems to be implemented in their jurisdiction. However, sensor/output collocation disparities may limit their ability to ever implement the control.

We are currently conducting searches for the following two remaining positions. Knowing the difficulty in finding faculty in these particular areas we started the searches last year and are on our second round of reviews. We have three individuals scheduled to interview for the Idaho Falls position in Idaho Falls January 8, 10, and 11. We have been conducting telephone interviews with candidates for the position in Moscow and expect to have on-campus interviews towards the end of January. These positions are:
- Assistant Professor in Computer Science in Idaho Falls; expertise in security in internet of things.
- Assistant/Associate Professor in Computer Science in Moscow; expertise in cyber security of cyber-physical controls systems.

II.1.B Graduate Students

Currently two graduate students, both in PhD programs, are working as research assistants under the project--Mohammad Ashrafuzzaman and Ananth A. Jillepalli. Both were hired at the beginning of fall 2017 semester. Mohammad was assisting Krishna Koganti (who graduated in summer 2017) with his work on the VMWare based Industrial Control Systems (ICS) Testbed project. Mohammad authored a paper based on this work that was accepted for the MALCON2017 conference. For his own research under this project, Mohammad is working on detecting and preventing stealthy cyber-attacks on cyber-physical power systems using deep learning techniques and cybernomics. He has started applying deep learning algorithms to detect false data injection attacks in power systems. The data-sets he is using are being generated by a MATLAB simulation by Dr. Yacine Chakhchoukh. Mohammad has presented the idea as a poster in the Pacific Northwest Industry Workshop and is now writing a paper for submission in a journal.

Ananth Jillepalli is developing a High-level and Extensible System for Training and Infrastructure risk Assessment (HESTIA) for cyber physical control systems (CPCS) infrastructure. Identifying vulnerabilities in a CPCS infrastructure can be challenging without a high-level security policy specification. Yet knowing the security policy specification is not sufficient to eliminate vulnerabilities. Knowledge of possible attacks and respective defense

measures are also needed to secure CPCS infrastructure. Ananth has also assisted Krishna Koganti in testing Krishna's Matlab-based ICS testbed. During his tenure as a research assistant in fall 2017 semester, Ananth has worked on several publications, a poster, and a lightning talk.

III.1.C Laboratory Enhancements

The most significant accomplishment with respect to laboratory enhancements is the expansion of the Power Applications Laboratory in Moscow. It underwent a major expansion from about 1,500 sq.ft. to 2,200 sq.ft. (Figure 1). In the original proposal we planned to use the existing space and just enhance the equipment in it. But we took advantage of an opportunity presented by the Murdock Foundation to invest an additional $285,000 of their funding invested in the laboratory with an additional $200,000 of other funding invested in Coeur d' Alene to create a distributed testbed with locations in Moscow, Idaho Falls, and Coeur d' Alene. We have worked with the Schweitzer Engineering Laboratory (SEL) Engineering Services Division to design this testbed for performing research on cybersecurity of power and industrial control systems. This testbed will enable research and development of novel and secure techniques and algorithms for securing today and tomorrow's Power Grid (PG) along with other types of Industrial Control Systems (ICS). The major advantage of this testbed is that it will enable researchers and engineers to perform and collaborate on ICS-specific cybersecurity research, development, and testing on a system that closely resembles current distributed critical infrastructure cyber-physical control systems. The testbed will expose hardware-in-the-loop simulation, enable the capture and use of real operational data, integrate current and future components of the power grid and other industrial control systems, and enable realistic attack-defend scenarios for research, evaluation, and testing. It will integrate with the current Real Time Digital Simulator (RTDS) and be accessible from the other UI locations as well as BSU. This capability will significantly enhance our ability to demonstrate (in-situ) advanced PG/ICS technology to Idaho industry partners.

The increased scope and capability of this change has come with a cost, in that the enhancements will take about 9 months longer than we originally anticipated. However, this is a small price to pay for the benefit we are gaining. The space for the test bed was remodeled and completed the end of November, two months behind schedule because of asbestos abatement in the new space. A contract was given to Schweitzer Engineering Laboratories for the industrial control equipment and RTDS upgrade. The equipment started to arrive in December, as shown in Figure 2. The RTDS and associated amplifiers were moved to the lab and test equipment was connected to the RTDS as shown in Figures 3-6. We will provide a more comprehensive description of the laboratory in the next, upcoming annual report.
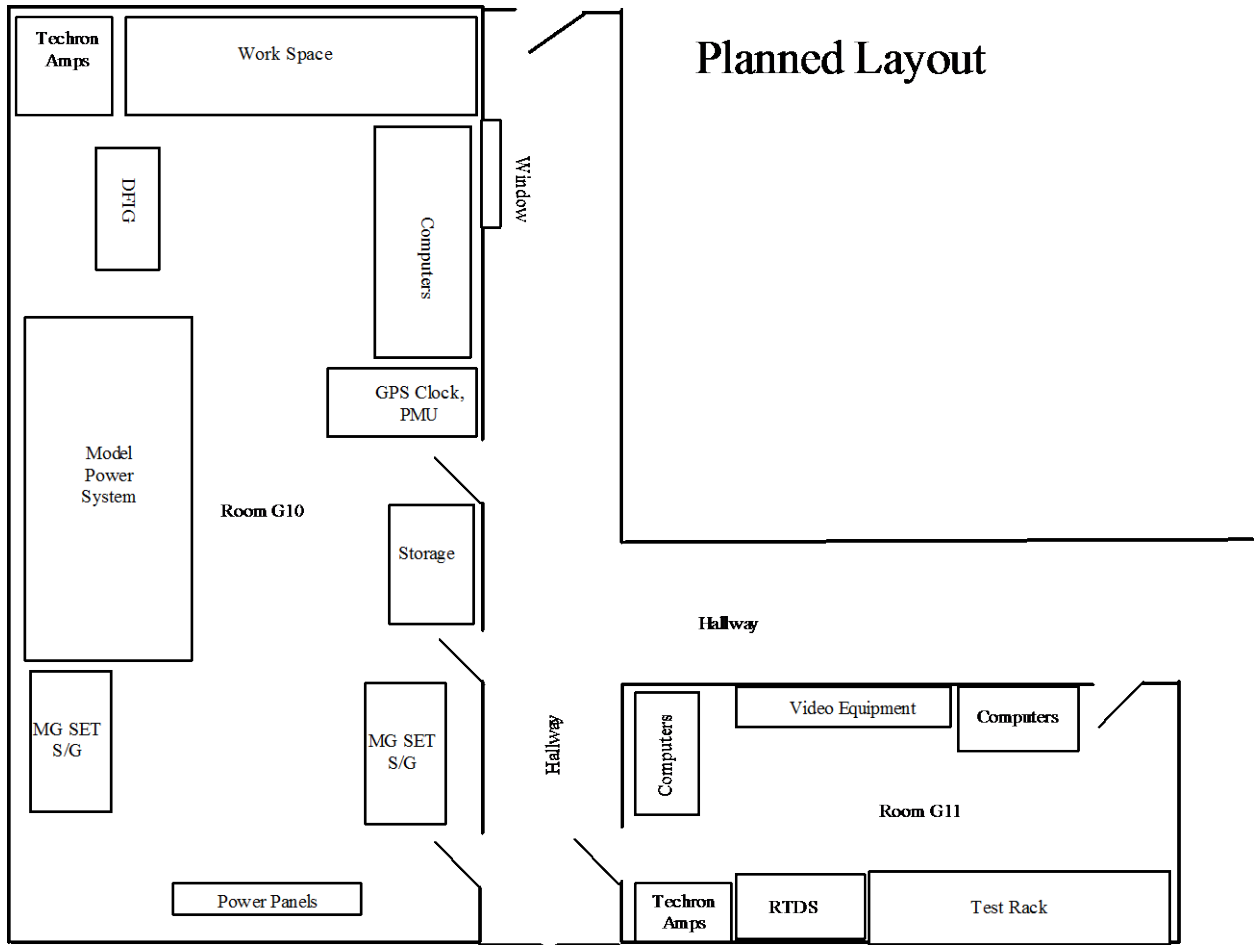
Figure 1: Illustration of Power Systems Laboratory Expansion

Figure 2: Some of the test equipment for the expanded power lab along with new equipment racks

Figure 3: Amplifiers moved and installed in the new space.

Figure 4: Some of the test equipment for the expanded power lab along with new equipment racks

Figure 5: RTDS, some of the test equipment racks and power amplifiers in remodeled lab space

Figure 6: Some of the test equipment for the expanded power lab along with new equipment racks

(2) Strengthen collaboration with Idaho industry and other Idaho universities

III.2. Industry and University Collaborations

Our team had numerous on-going and one-time collaborations with industry and other universities. Some of these collaborations are listed below:

Brian Johnson has had weekly meetings with Craig Rieger and Tim McJunkin from the INL related resilient control of critical infrastructure. Efforts included:
(1) Ongoing research project as part of DOE Grid Modernization Lab project related to resilience metrics for power distribution systems.
(2) Collaboration on an ongoing LDRD proposal related to cybersecurity for industrial control systems, with collaboration from Virginia Commonwealth University.
(3) Collaboration course ECE 469/569: Resilient Control of Critical Infrastructure with collaboration between UI, BSU, and INL along with some interaction with Naval Post Graduate School, Weber State University, and Idaho State University.

Brian Johnson had monthly meetings with engineers from ABB Corporations, University of Illinois, Argonne National Lab and Bonneville Power Administration as part of a project addressing cybersecurity for HVDC transmission systems.

Brian Johnson and Yacine Chakhchouhk have been part of a project with Avista Corporation looking at non-wire solutions that use sensors and controls to alleviate the need for new transmission lines to improve reliability of power systems at a lower cost.

Brian Johnson was advisor for three industry sponsored senior design teams, one sponsored by Avista and one by Schweitzer Engineering Laboratories.

Yacine Chakhchoukh is having regular meetings with professors at Virginia Tech (Lamine Mili, Michael von Spakovsky, and Konstantinos Triantis). The team is writing a joint proposal with other professors at other universities to submit in March 2018 to the NSF. The title is: "Enhancing the resilience of interdependent power systems and emergency services via micro-grids" targeted starting date August 2018. For this project the cyber-security test-bed will be used in the research conducted at the University of Idaho. Collaboration will be started with AVISTA Corporation on this project.

Date: September 18, 2017: Visit and presentation: **Visitor/Speaker:** Dr. Svitlana Volkova, Senior Research Scientist, Data Sciences and Analytics Group, National Security Directorate, Pacific Northwest National Laboratory (PNNL). **Title:** Topic: Predicting the Future with Deep Learning and Signals from Social Media. Also, Dr. Volkova and a research and recruiting team from PNNL visited the University of Idaho and met with students and faculty.

Date: October 09, 2017: Visit and presentation: **Visitor/Speaker:** Ginger Wright, Program Manager for Domestic Nuclear Cybersecurity at Idaho National Laboratory (INL). CS Colloquium presentation, **Title:** Cyber Informed Engineering. Ms. Wright also met with College of Engineering faculty and students.

Date: November 27, 2017: Visit and presentation: **Visitor/Speaker:** Dr. Glenn A. Fink, Senior Cyber Security Researcher, Pacific Northwest National Laboratory (PNNL). CS Colloquium presentation, **Title:** Security and Privacy Grand Challenges for the Internet of Things. Dr. Fink also met with College of Engineering faculty and students.

Date: November 27, 2017: Presentation: **Visitor/Speaker:** Jason Dearien, Senior Application Engineer, Schweitzer Engineering Laboratories (SEL), **Title:** Requirements and Challenges of Building Software for Critical Infrastructure. Mr. Dearien also met with College of Engineering faculty and students after the presentation.

Date: Fall, 2017: Live Table Top Exercise: **Visitor/Speaker:** Dr. Jessica Smith, Cybersecurity Researcher, Pacific Northwest National Laboratory (PNNL), helped organize and participated in a critical infrastructure cybersecurity event tabletop exercise for University of Idaho students.

Date: Fall, 2017: Engineering Capstone Design Projects. **Customer:** Dr. Jessica Smith, Cybersecurity Researcher, Pacific Northwest National Laboratory (PNNL), is sponsoring two College of Engineering Capstone Design projects focused on cybersecurity of the Power Grid and Industrial Control Systems.

(3) Foster technology transfer and commercialization through technology incubation
During the past six months we have had several proposals accepted and submitted for research in this area.

III.3.A Proposals

ACCEPTED

H.L. Hess, B. Johnson, Y. Chakhchoukh, "Framework for Siting and Sizing Energy Storage for Enhanced Performance of the Avista System," Avista Corporation, August 15, 2017 - August 31, 2018, $83,712.89.

A. Ibrahim, B. Rezaie, B.K. Johnson, "Aerogel Insulation System: An Innovative Energy Efficient Thermal Wall," Avista Corporation, Sept. 1, 2017- August 30, 2018, $88,777.

B.K. Johnson, Y. Chakhchoukh and D. Conte de Leon, "Testbed for Power and Industrial Control Systems," Murdock Charitable Trust, May 18, 2017-August, 31, 2019, $284,500 (total project $872,407)

SUBMITTED

B.K. Johnson, H.L. Hess, Y. Chakhchoukh (all University of Idaho), Craig Rieger (INL, and Milos Manic (Virginia Commonwealth University, Real-time Sensing of Transient Occurrences through Resilient Design (ReSTORD), Bonneville Power Administration, $459,588

B.K. Johnson, H. Lei, Student Support for the 2018 International Conference on Probabilistic Methods Applied to Power Systems, National Science Foundation, $12,750

Title: SaTC: EDU: Development of Reverse Engineering Laboratory and Curriculum
Amount Requested: ~$ 300,000
Proposed Period: October 1, 2018 to September 30, 2020 (2 years).
Proposed Source: NSF, Secure and Trustworthy Cyberspace, Education: SaTC:EDU.
Location: University of Idaho, Idaho Falls, Idaho, U.S.A.
PI: Haney, Michael; Computer Science, Idaho Falls, University of Idaho.
CoPI: Roberson, Dakota; Electrical and Comp. Engineering, Idaho Falls, University of Idaho

Title:
SaTC: CORE: Small: Cybersecurity Analysis of PMU-based State Estimation for the Smart Grid
Amount Requested: $ 499,982
Proposed Period: August 20, 2018 to August 19, 2021 (3 years).
Proposed Source: NSF, Secure and Trustworthy Cyberspace, SaTC, CORE Program.
Location: University of Idaho, Moscow, Idaho, U.S.A.
PI: Chakhchoukh, Yacine; Electrical and Computer Eng. Moscow, University of Idaho.
CoPI: Conte de Leon, Daniel; Computer Science, Moscow, University of Idaho.
CoPI: Johnson, Brian K.; Electrical and Computer Eng. Moscow, University of Idaho.

III.3.B Publications

PUBLISHED or ACCEPTED

Conte de Leon, Daniel; Stalick, Antonius Q.; Jillepalli, Ananth A.; Haney, Michael A.; Sheldon, Frederick T. (2017) "*Blockchain: Properties and Misconceptions*", Asia Pacific Journal of Innovation and Entrepreneurship, Volume: 11 Issue: 3, pp. 286-300, December 2017. https://doi.org/10.1108/APJIE-12-2017-034.

Conte de Leon, Daniel; Brown, Matthew G.; Jillepalli, Ananth A.; Stalick, Antonius Q.; Alves-Foss, Jim. *"High Level and Formal Router Policy Verification."* The Journal of Computing Sciences in Colleges, Volume 33, Number 1, pp. 118, October 2017. https://dl.acm.org/citation.cfm?id=3144631

Jillepalli, Ananth A.; Sheldon, Frederick T.; Conte de Leon, Daniel; Haney, Michael A.; Abercrombie, Robert K. "*Security Management of Cyber Physical Control Systems Using NIST SP 800-82r2*". In Proceedings of the 13th International Wireless Communications and Mobile Computing Conference (IWCMC), 26-30 June 2017, Valencia, Spain, IEEE. DOI: 10.1109/IWCMC.2017.7986568http://ieeexplore.ieee.org/document/7986568/

Conte de Leon, Daniel; Goes, Christopher; Jillepalli, Ananth A.; Haney, Michael A.; Krings, Axel. "*ADLES: Specifying, Deploying, and Sharing Hands-On Cyber-Exercises*", Journal of Computers and Security, To Appear, Elsevier 2018. https://www.journals.elsevier.com/computers-and-security

Jillepalli, Ananth A.; Conte de Leon, Daniel; Sheldon, Frederick T.; Haney, Michael A. "*Hardening the Client-side: A Guide to Enterprise-level Hardening of Web Browsers.*" In Proceedings of the 15th IEEE International Conference on Dependable, Autonomic and Secure Computing (IEEE DASC 2017). November 2017. IEEE.

Koganti, Venkata SreeKrishna; Ashrafuzzaman, Mohammad; Jillepalli, Ananth A.; Conte de Leon, Daniel; Sheldon, Frederick T.; *"A Virtual Testbed for Security Management of Industrial Control Systems."* In Proceedings of the 12th International Conference on Malicious and Unwanted Software (MALCON 2017). November 2017. IEEE.

S. Basumallik, S. Eftekharnejad, N. Davis, N. Nuthalapati, B.K. Johnson, "Cyber Security Considerations on PMU-base State Estimation," *Proceedings of the 2017 Cybersecurity Symposium.* Coeur d'Alene, Idaho, April 17-18, 2017

P. Penkey, H. Samkari, B.K. Johnson, H.L. Hess, "Voltage Control by Using Capacitor Banks and Tap Changing Transformers in a Renewable Microgrid," 2017 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), April 23-26, 2017, Arlington Virginia

N. Fischer, B.K. Johnson, J.D. Law, A.G. Miles, "Induction Motor Modeling for Development of a Secure In-Phase Motor Bus Transfer Scheme," 2017 IEEE International Electric Machines and

Drives Conference (IEMDC), Miami, FL May 22-25, 2017. Reviewed based on extended abstract)

N. Fischer, J.D. Law, A.G. Miles, B.K. Johnson, "Dynamic Modeling of an Improved In-Phase Motor Bus Transfer Scheme," *Proceedings of the International Conference on Power Systems Transients (IPST2017)*, Seoul, South Korea, June 26-29-18, 2017.

Anujan, B.K. Johnson, E.J. William, "Protection Studies of Geographically Dispersed Type 3 Wind Energy Systems," *Proceedings of the 2017 IEEE Power and Energy Society General Meeting*, Chicago, IL, July 2017

S. Chilukrui, M. Alla, B.K. Johnson, "Enhancing backup protection for thermal power generating stations using sampled values," *Proceedings of the 2017 North American Power Symposium,* Morganton, WV, September 17-19, 2017.

S. Basumallik, S. Eftekharnejad, N. Davis, B.K. Johnson, "Impact of false data injection attacks on PMU-based state estimation," *Proceedings of the 2017 North American Power Symposium,* Morganton, WV, September 17-19, 2017.

H. Beleed and B.K. Johnson, "Comparative study on IEEE12 bus system with D-FACTS devices in different simulation tools," *Proceedings of the 2017 North American Power Symposium,* Morganton, WV, September 17-19, 2017.

W. Parker, B.K. Johnson, C. Rieger, T. McJunkin, "Identifying critical resiliency of modern distribution systems with open source modeling," *Proceedings of Resilience Week 2017.* Wilmington DE, September 19-21, 2017

V. Koganti, M. Ashrafuzzaman, A. Jillepalli, F.T. Sheldon, B.K. Johnson, "A Virtual Testbed for Security Management of Industrial Control Systems," MALCON 2017, Malware Conference, January 2018, San Juan, Puerto Rico (delayed due to hurricane damage)

SUBMITTED

Jillepalli, Ananth A.; Conte de Leon, Daniel; Sheldon, Frederick T.; Haney, Michael A. *"Enterprise-level Hardening of Web Browsers."* Submitted to Springer Security Informatics Journal. https://security-informatics.springeropen.com/

Steiner, Stuart; Jillepalli, Ananth A.; Conte de Leon, Daniel; *"Applying the Principle of Least Privilege to Harden Web Application Security."* Submitted to Springer Security Informatics Journal. https://security-informatics.springeropen.com/

Jillepalli, Ananth A.; Conte de Leon, Daniel; Sheldon, Frederick T.; Chakhchoukh, Yacine; Johnson, Brian K.; Haney, Michael A. *"An Architecture for HESTIA."* Submitted to 24th National Conference on Communications (NCC 2018). February 2018. Hyderabad, India.

Steiner, Stuart; Jillepalli, Ananth A.; Conte de Leon, Daniel; *"Hardening Web Applications Using a Least Privilege DBMS Access Model."* Submitted to 24th National Conference on Communications (NCC 2018). February 2018. Hyderabad, India.

IN PREPARATION

Jillepalli, Ananth A.; Conte de Leon, Daniel; Bhandari, Venkata A.; Steiner, Stuart; Alves-Foss, Jim *"Analysis of Web Browser Security Configuration Options."* To be submitted to IEEE Access Journal. http://ieeeaccess.ieee.org/

Ashrafuzzaman, Mohammad; Jillepalli, Ananth A.; Chakhchoukh, Yacine; Conte de Leon, Daniel; Sheldon, Frederick T.; "*Detecting Stealthy False Data Injection Attacks in Smart Grid Using Deep Learning"*. To be submitted to Future Generation Systems Journal.

III.3.C Presentations
 Title: Application of Protection Challenges for Connecting to a Microgrid
Place**:**   Idaho Commons.
                 Co-sponsored by the IEEE Palouse Section and the University of Idaho.
Date&Time: September 14, 5:00pm
Speaker: John Kumm, P.E., POWER Engineers.

Title: Traveling Wave Technology for Accurate Fault Location and Ultra-High Speed Line Protection
Place: Schweitzer Engineering Laboratories Event Center.
                 Co-sponsored by the IEEE Palouse Section and the University of Idaho.
Date&Time: September 25, 6:00pm
Speaker: Venkat Mynam, Principal Research Engineer, Schweitzer Engineering Laboratories, Inc.

Title: Remedial Action Scheme Preventing Country-Wide Blackout
Place: Idaho Commons, University of Idaho.
                 Co-sponsored by the IEEE Palouse Section and the University of Idaho.
Date&Time: October 10, 6:00pm
Speaker: Brian Clarke, P.E., Automation Engineer, Schweitzer Engineering Laboratories, Inc.

Title: Smart Cities for Promoting Global Sustainability
Place: Washington State University.
                 Co-sponsored by the IEEE Palouse Section and the University of Idaho.
Date&Time: November 7, 11:00am
Speaker: Mohammad Shahidehpour, University Distinguished Professor, Bodine Chair Professor of Electrical and Computer Engineering, and Director of the Robert W. Galvin Center for Electricity Innovation at Illinois Institute of Technology (IIT)

(4) Strengthen and expand the workforce

In our proposal we stated that accomplishments in this Objective would not occur until year 3. However, our team has already made some progress, namely:

III.4.A Student Internships

1. INL: Four Cybersecurity students participated in internships at Idaho National Laboratories during the summer of 2017. These students worked on projects related to the cybersecurity with a focus on industrial control systems and critical infrastructure protection.

2. PNNL: Three Cybersecurity students participated in internships at Pacific Northwest National Laboratory during the summer of 2017. These students worked on projects related to the cybersecurity of industrial control systems.

III.4.B Cybersecurity Competitions and Student Professional Development

1. November, 10-11, 2017: NICCDC: NIATEC Collegiate Cyber Defense Competition, Pocatello, Idaho: Eight University of Idaho students (7 from Moscow and 1 from Idaho Falls) traveled and participated in this live cyber defense competition organized yearly by NIATEC at Idaho State University.

IV. Description of Future Project Plans

Plans for the future are to accomplish the deliverables of the four objectives. Specifically for the second half of year one we plan to:
- Complete the hires of listed in III.1.A above.
- Complete the enhancements to the Power Applications Laboratory. This task has been expanded by the additional funding from the Murdock Foundation.
- Host the Cybersecurity Symposium 2018, April 9-11 in Coeur d' Alene, organized by the University of Idaho and sponsored by the Center for Secure and Dependable Systems in the College of Engineering.
- Co-sponsor the June 2018 Probabilistic Methods in Power Systems Conference in Boise, Idaho.
- Place six student interns in industry this coming summer to develop demonstrations for the distributed test bed.